

ئەم كاتەتەن باش ھاورپىيان

پىنھەمكى

سوپاسى خوداى گەورە دەكەم كە ئەم دەرفەتەى پىدام بۇ بەخشىنى كەمىك لەو راتانەى كە كۆم كروونەتەو و پىشكەشى ئىوەى دەكەم تىنشاالله.

كورتەمەك دەربارەى راتەكان RATs

رات چى يە؟

بەرنامەيەك Software ئىكە ھەر ھەك پۇلى بەرنامە ئاسايەكانى دىكە ، بەلام بەكار و پىشەى جودا ، ھەلدەستىت بە دەستبەسەراگرتن Remote كردنى ھەگەرخەر Operator ئىك.

شېوازى كاركردنى راتەكان فېزىكائە Physical Access ، واتە شېوازىكى خودكارانەى ھەيە و دەتوانىت بىلاويىتەو بەسەر سىستەمدا و جىگىر بىيىت لەسەر فائىلەك بەنموونە ، ھەر ئەم تايەتەتەندىەى واپىكردووە كە زۆرجار فائىلەكانى دىوى سىرغەر -Server Files- پىنى بگوترىت -Trojan- تروچان.

تروچان چى يە؟

ئەگەر بەشېوہەيەكى درووست لە راتەكان بېروانىن ، دوو مېتۇد بەرئوہى دەبات :

1. فائىلى ھاپپىچ و درووستكراوى (Client).

2. فائىلى ھاپپىچ و درووستكراوى (Server).

بەلام كاتىك ھەردوك فائىل بەھۇى بەرنامەيەكى ھەكو رات -RAT- دەبەستىت بەيەكەوە ئەوكات دەتوانىن پىنى بلىن -Trojan- كەواتە فائىلى ھاپپىچى دىوى (Client + Server) پىكەوە تروچانىك درووست ئەكەن كە بەھۇى رېرەوئىكەوە -DNS- داتا ئالوگۇر دەكات ، ھەمەركات Domain Name System پىشكىش بە فائىلەكە كرا ئەوكات تروچان دەيئە (Trojan Horse) واتە (ئەسپى تروچىن) ، لىرەدا ئەسپەكە دۆمەينە ھەك No-IP كە يارىدەى جىگىركردنى ئايپى دەدات بەھۇى دامەزراوہەيەكى سىستەم لەسەر ھۇستىك ياخود ئايپەك . بەكورتى فائىلە ھاپپىچكراوہ دوانىيەكە تروچانە و ھۇستەكەش لەسەر دۆمەينىك (DNS) ئەسپە كەيەنەرەكەيە.

لىرەدا پرسىارىك درووست دەيىت: ئايا راتەكان تەنھا بۇ مەبەستى ھاك كەردن بەكار دىت؟

نەخىر ، راتەكان لەبنەرەتدا بەرنامەى ھاك لىن تا ھاكەر ھاكى پى بكات ، بەلكو تەنھا بەرنامەى فېركارىن لەبۇ فېركەكان . بەلكو بەھۇى راتەكانەوە كەشەپىدەر ئەك ھاكەر ، تروچانىك ھاپپىچ دەكات و بەكارى دىيىت بۇ دەستبەسەرا گرتن.



شېوازى كەللەسەرى سەربازىكى جەنگى تەروادە (يۇنان)

لە بوارى ھاكىشدا يۇنان -گريك-

مىژووى تروچان ، جەنگى تەروادەمان بىر دەختەوە كاتىك بۇ تۆلەسەندەوە ھىكتۇرى پادشا ، چوو تۆلە بىستىنئەوە لەبرى نامۇزا كوزراوہەكى لە يۇنان ، بەلام سەربازى كەم بوو ، ئاچار پلانىكى دارشت بۇ ئەوہى زەبرىكى توند بدات لەدوژمن ، ھەربۇيە تروچانى درووست كەرد ، ئەم رووداوہ گرىكە بۇ ھاكەران.

دواتر ھىكتۇر ھات ئەسپىكى درووستكرد بە تەختە و پرى كەرد لە سەرباز و بەدىارى ئاردى بۇ پادشاى دوژمن ئەم ئەسپە ئەوئەندە زەبەلاح بوو ھەموو خەلكى شار سلىان دەكردەوہ ، لەشەودا بوو ئەسپەكە بە پال پىوہەنان بەھۇى رەوەرەوہ -تايە- كانىوہ تايەيانى دواتر برا بۇ ناو شارى دوژمن ، و كرا بەدىارى ، بەلام لەنيوہشەودا سەربازانى ناو ئەسپەكە بەجاريك خۇيان ھاويشتە دەرەوہ و دايان بەسەر شاردا و تەفرو تونايان كەرد.

بەم شېوہە بەھۇى تروچانىكەوە (فائىلىكى ھاپپىچ) دەستگىرا بەسەر ھەگەرخەرى شار (سىستەم)ى دوژمن.



وونىئەى كىشراوى ئەسپى تەروادە (Trojan Horse)

روونكردنەوہى وونىكە:

خەلكەكە: (Victim-كەسى قورىانى)

تايەكان: (Link-لىنك)

سەربازەكانى ناوى: (فابىرۇسەكان)

نامەكى ھىكتۇر و كرىكارەكان: (دەمچ binder)

شارەكە: (سىستەم system)

پەت (گورىسەكان): (كىك-Mouse Click)

سىاستى ھىكتۇر: (RAT-ئامانچ-Aim)

سىستەمى دوژمن

RAT: Remote Access Tool ، خەلك دوو جۇر بەكارى دىيىت:

1. تروچانىك درووست دەكات و دەپكاتە شارى دوژمن ، ياخود سىستەمى دوژمن (ئەگەر دوژمنىت ھەيە ئەوہ بەكە بۇى).

2. دوو فائىلى ھاپپىچى درووستكراو ، سىرغەر و كلىنت ، بۇ مەبەستى فېركارى لە دام و دەزكا كۆمەيەكان و قوتابخانەكانى ئايىتى دا.

ئىشى راتەكان بەگىشتى

دەتوانىن ئىشى راتەكان دابەش بەمىت بەسئ لىقەوہ:

ا. راتى مەبەست دار: مەبەست لەم جۇرە راتە ئەوہە كە كەشەپىدەر (Developer) بۇخۇى بەزمانىك راتىك درووست دەكات كە تەنھا مەبەست لىنى يەك جۇر ئىشە بۇ سەر كارپىكراوى قورىانى (Access Victim) و دەپەوئت تەنھا يەك كار بكات ، بەزۇرى سىخۇرەكانى بوارى پاراستن ئەم جۇرە لەرات درووست دەكەن تەنھا بۇ يەك مەبەست.

ب. راتى بى مەبەست: بىرئىيە لەو دوو فائىلە پەستىنراوہ ھاپپىچەى كە بۇ ھىچ مەبەستىكى دەست بەسەرا گراتن بەكار نايەت ، چونكە ئەگەر مەبەستداربىت كەواتە كەسانى ھاكەر بەكارى دەبەن ، وە ئەم جۇرە تەنھا لەتۇرى ئاوخۇپى دا كارى پى دەكرىت ، ھەك فېركەكان.

ج. راتى كىشت: ترسپنەرە و ھاكەر بەكارى دەبات و دەپكات بەتروچان ، كە بەراتى (RAT through a network connection) ئاسراون ، ئەمەيان قەسە زۇر ھەلدەكرىت بەلام بەگىشتى ئىشەكانى دەكەين بە چەند بەشكىەوہ:

1. دەست دەكرىت بەسەر كامپىرادا.

2. داتاكان ئالوگۇر دەكات.

3. شىل كەردن (ئىشى CMD).

4. ئىشەكانى ھاردويز (پارچە رەقەكان) دەكات.

5. رىجستەرى (داتا شارواہەكانى سىستەم)

6. ھىرش كەردن (Attack)

7. دامەزراندنى نەرمەكالا (Software)

8. رىموت كەردنى دىسكۇپ.

9. تاسك مانجەر بۇ داخستن و كەردنەوہ.

10. .. ھەتد.

راتەكان پىوئىستان بە چى ھەيە؟

بۇ ئەوہى بەباشى راتىك بەتايىتەتتى جۇرە كىشەكەى ، جىگىر بەمىت لەسەر سىستەمەكەت پىوئىستە رەچاوى ئەم خالانە ھەك ياسا بەمىت

ھەتاوہكو بەباشى راتىكى نەموونەى كىشتى بەكاربەئىت و ئىش بكات بەبى كىشە. خالەكان ياخود ياساكان:

1. لەرووى سايكۇلۇزىەوہ (دەروونى)

كەسىتى تۇ پىوئىستە پىش ئەوہى راتىك بەكاربەئىت ، دەروونى خۇت بناسىت ، تا ئەگەر بىت و كەسىتى شىلگىر و تۆرە بىت پىم واپە خراپە رات بەكاربەئىت ، چونكە دواجار بەزەرە و زىانى خۇتدا دەشكىتەوہ و ئەوئەندەى تر بارى دەروونىت لاواز دەيىت ، بۇيە كەسىتى خۇت زۇر كرىكە.

2. ئامانچ

فېربوونى راتەكان بۇ ئامانچە ، ھەتا ئامانچىك نەيىت وا باشترە خۇت فېر نەكەيت ، خۇ ئەگەر بەبى ئامانچ رات بەكاربەئىت ئەوا باشترە ، چونكە بۇ پۇلى دوومىت لە جۇرى راتەكان (تەنھا خۇت فېر دەكەيت).

3. راتىك دەستىشان بەكە

زۇر بەگەرى ھەتا راتىك دەدۇزىتەوہ كە زۇر سەرنجىت رادەكىشىت ، بۇ پرىسار لەكەسانى بەنەزموون بەكە ، خۇت بەگەرى ، دواجار راتىك دەستىشان بەكە و بىكە بە ھاورپىت بەلنى (My RAT Friend for Ever) من ھاورپىيەكە ھەيە زۇرم خۇش دەوئىت و زۇرىش نەيىيە ، لە كۆمپىوتەرەكەمدايە ، ھەركات كە دەپكەمەوہ ئارامى بە دلىمدا دىت ، ئەگەرچى ئەو ھاورپىيەشم ھىچم پىشكەش ناكات.

4. رات چى يە؟

ئەك رات RAT ، بەلكو رات چى يە دەربارەى ھاورپىكەت RAT ؟ ئەم پرىسارە ھەك ئەوہ واپە بلىنى: من كىم؟ دەى كەواتە بەگەرى بزانە رات چى يە بەرامبەر بە RAT ؟

5. دەركاكەى لى بەكرەوہ

Port دەركە و دەرچەيە ، پۇرت بەكرەوہ ، ھەرچۇنىك بىت تۇ دەبىت نان بەدەيت بەھاورپىكەت تا ئەوئىش سودت پى بەكەيەنىت.

6. DNS دابەمىزئىنە

ناكرىت و ئاشىت ھەرچى ئىشنىك كە ھاورپىكەم RAT بۇم دەكات بچىت بۇ تۇ! ، كەواپە راتكەت توندوتۇل بەكە و ئايپەكەت جىگىرى بەكە بەھۇى دۆمەينىكەوہ با ئەو ئىشەى راتەكە دەپكات بىتەوہ بۇ ئەمرەكەى تۇ.

7. تاقىكردنەوہ باشترىن بەلگەيە

سىستەمىكى تاقىكارى (تافىكە) دابەمىزئىنە بەخەيانى (Virtual System)

8. وورىابە (ئاگاداربە) (Warning)

ھەندىك جار راتەكانىش بى وەفان ، بەگەرى و لەكۇتايدا ئەمەت بۇ دەرەكەوئىت.

9. ئىستاش خانى يەكەم سەير بەكرەوہ؟!

(من راتە كىشەكان بەكار ئاھىنم چونكە زۇر كەسىكى ھەنچوم)

وەرە راتىك بەكە بەھاورپىت

لەجىھاندا زۇر راتى كىشتى (Public) ھەن كە تونايپا بى سنوورە لەدەست بەسەرا گرتن ، وە تۇ تاكو ئىستاش ھاورپىيەكى بەنرخت نپە ، چونكە گومانە ھەيە ، ئەوئە لىرە كۆمەنىك راتى جىاواز دەبىيىت ، وە لەوانىيە تۇش بى وەفا دەرچىت بەرامبەر بەراتە كۆنەكەت.

بەھەرحال زۇرىك گەراوم و زۇر ماندو بووم تاكو تونايم ئەم راتانە كۆبەمەوہ و لە بابەتىكدا بۇ ئىوہى خۇشەويستى دابىنم .

تېيىنى:

زۇربەى ئەورائانەى لەبەشى (راتەكان - RAT) ھەيە دام نەنانون ، تۇ دەتوانىت لەوئى ھاورپىيەك دەستىشان بەكەيت.

ھەك بۇ كورد

سەرچاوەماك بۆ دەست گەوتنى زانیاریەكان

A source for getting information

راتەكان - RAT

تېيىنى دووہم:

لەسەرەوہ ناو وە وونىنە و ژمارەى راتەكان دادەنىم ، چونكە فېركارىيەكە وونىيە ، و لەخوار وونىئە RATەكانەوہ ئەگەر راتىك بەدل بوو دەتوانى بەژمارى وونىكەيدا لەخوارەوہ دايىگىرىت.

تېيىنى سېھەم:

مەبەست لەو راتانەى كە دامناوہ ، زياتر بۇ ئەوہە ئاشناپى لەكەل جۇرى راتەكە بەكەين ، وە دەتوانىت لەھەر شوئىنىكى مەمانەپىكراو فېرشنى نوئى تر ئەگەر ھەبوو وەر بگىرىت.

لە كۇتايى دا

سوپاس و ستايىشى خوداى گەورە دەكەم كە ھانى دام بۇ تەواو

كەردنى بابەتەكە و سوپاسى بەرئوہەرى ئەم يانەيە (ھەنگاو ھەولپىرى)

دەكەم كە كەمەك يارمەتتى دام ، و سوپاسى ئەندامان و

سەپەرشتىاران دەكەم.

چەند شتىك ھەيە پىوئىستە لە بەشى كۇتايى دا بىلنم ، دەمەوئىت سەبارەت بە كورتكراوہى RAT ئامازە بدەم ، زۇرىك لە شوئىنە گرىك و بەنەزموونەكان درىژكراوہى RAT بە چەند شېوہەك دىتە ناو جىھانى

چەمكەكانى كۆمپىوتەرەوہ ، جا بەكارھىنەر دەتوانىت چەمكىك بكاتە سەر بنەرەتتى كورتكراوہەك ، لەوانە:

- بەھۇى ئەوہى لەبواری ھاكدا زۇرىك لە بەكاربەرانى رات بۇ مەبەستى دەستبەسەرا گرتن و بەرئوہەبردن بەكارى دەھىنن كەواتە

لىرەدا RAT كورتكراوہەكى بەم شېوہەيە (Remote Administration Tool) ياخود لەبەر ئەوہى تەنھا يەك تۈول نپە ئەوا (Remote Adminis-

tration Tools).

- سەبارەت بەجۇر و شېوہى بەكارھىنانى راتەكان رېرەو و

بۇچونىكى دىكەش ھەيە لەسەر چەمكى پات ، دەكرىت بلىن ئەم

درىژكراوہەيە بۇ ھاكەر ئاشىت ، چونكە ھەرسى جۇرى راتەكان

دەكرىتە خۇ ، ئەوئىش (Remote Access Tool) ياخود (Remote Access Tools).

- ھەر لەبواری كۆمپىوتەر و نىت وۇركدا چەمكىكى تر ياخود

درىژكراوہەيەكى ترى RAT ھەيە ئەوئىش (-Remote Access Technology)

og) كەبۇ دەستبەسەراگرتنى پارچە رەقەكانى سەر تۇرىكى ئاوخۇپى

يان دەرەكى دەيىت و ئەم درىژكراوہەيە بەكار دەبرىت لە دام و دەزكا

كۆمەيەكاندا.

- بەرنامەى (Robust Audio Tool) بەھەمان شېوہ كورتكراوہەكى

RAT ، كەبۇ بواری میديا و دەنگ بەگىشتى بەكاردىت.

- وە دواجار RAT بە جىج ياخود مشكى زۇر گەورە دەگوترىت.

ئەم بابەتە وونىئەى فېركارى بە دوو شېوہى جودا دادەنىم تا لاى تۇى

خۇيىنەر مەيىتەوہ ، بە شېوہى pdf و شېوہى jpg وە بەدەر لەوہى

راستەوخۇ لەبەرەدەت حازرە.